Pemenuhan Prinsip *Shannon* (Difusi dan Konfusi) dengan Fungsi $f(x) = 10x$ pada Kriptografi *Block Cipher* dengan Pola Garis Pertumbuhan dan Pita Pertumbuhan Cangkang Kerang

[1]Christin Marcelin Dias, [2]Magdalena A. Ineke Pakereng, [3]Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1]672009080@student.uksw.edu, [2]ineke.pakereng@staff.uksw.edu,
[3]alzdanny.wowor@staff.uksw.edu

Abstract

Block cipher with Garis Pertumbuhan dan Pita Pertumbuhan Cangkang Kerang (GPCK) pattern algorithm is developed based on the transposition process with a block size of 64 bits. GPCK already meet some of the test such as the value of data randomness and differentiation, but do not meet the principles in the block cipher like Shannon principle (Diffusion and Confusion) and iterated cipher. This study modifies GPCK algorithm using the function f(x) = 10x which is used to generate constants as additional processes on modification made to meet the principles iterated cipher by reaching saturation levels with twenty rounds. Value avalanche effect obtained after each round of modifications vary, but on average increased by 19.45%. the use of the function f(x)=10x into a central role in increasing the value of the avalanche effect significantly to the fulfillment of the principle of Shannon.

Keywords: *Block Cipher, Garis dan Pita Pertumbuhan Cangkang Kerang, Cryptography, Principles of Shannon, Iterated Cipher, Avalanche Effect, f(x) = 10x.*

Abstrak

Blok *cipher* dengan pola Garis Pertumbuhan dan Pita Pertumbuhan Cangkang Kerang (GPCK) merupakan algoritma yang dikembangkan berdasarkan proses transposisi dengan ukuran blok sebanyak 64 bit. GPCK sudah memenuhi beberapa pengujian seperti nilai keacakan dan diferensiasi data, tetapi belum memenuhi prinsip dalam *block cipher* seperti prinsip Shannon (Difusi dan Konfusi) dan *iterated cipher*. Penelitian ini memodifikasi algoritma GPCK menggunakan fungsi $f(x) = 10x$ yang digunakan untuk membangkitkan konstanta sebagai proses tambahan pada modifikasi algoritma. Hasil yang diperoleh menunjukkan bahwa modifkasi yang dilakukan dapat memenuhi prinsip *iterated cipher* dengan mencapai tingkat jenuh dengan dua puluh putaran. Nilai *avalanche effect* yang diperoleh setelah modifikasi bervariasi tiap putaran, tetapi secara rata-rata meningkat sebanyak 19.45%. Penggunaan fungsi $f(x) = 10x$ menjadi peran sentral dalam peningkatan nilai *avalanche effect* secara signifikan guna pemenuhan prinsip Shannon.

Kata Kunci : Blok Cipher, Garis dan Pita Pertumbuhan Cangkang Kerang, Prinsip *Shannon, Iterated Cipher, Avalanche Effect, f(x) = 10x.*

---

[1] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga.
[2] Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.
[3] Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.